Enterprise Income Verification (EIV) System
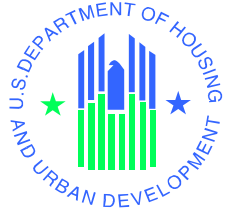
Security Administration Manual

U.S. Department of Housing and Urban Development

March 2006

Revision History

Version	Date	Comments required	Approvals required
Version 1.0	09/16/05	Build 4.0 Release	
Version 2.0	03/10/06	Build 5.0 Release	

Enterprise Income Verification – Security Administration Manual Authorization Memorandum

I have carefully assessed the Security Administration Manual for the Enterprise Income Verification (EIV) system. This document has been completed in accordance with the requirements of the HUD System Development Methodology.

MANAGEMENT CERTIFICATION - Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____   _____
David Sandler   Date
IT Project Manager

_____   _____
Nicole Lawyer   Date
PIH Program Manager

_____   _____
Lanier Hylton   Date
MF Housing Program Manager

Table of Contents

List of Figures

1 Preface

1 Preface

1.1 Document Overview

The purpose of this manual is to provide instructions for HUD personnel (Office of Public and Indian Housing and Office and Housing) responsible for security administration in the Enterprise Income Verification (EIV) application. It details business operational procedures for successfully performing administration tasks through EIV user interface.

1.1.1 How This Manual is Organized

Listed below are each of the chapters contained in this manual, along with a brief description of its content:

- **Chapter 1, Introduction** – An overview of EIV, including the hardware, software, and system architecture.

- **Chapter 2, PIH Security Administrators** – Provides instruction on the functions available to PIH Security Administrators.

- **Chapter 3, Multifamily Housing Security Administrators –** Provides instruction on the functions available to Multifamily Housing Security Administrators.

- **Appendix A, Abbreviations and Acronyms** – Provides a list of commonly used abbreviations and acronyms.

1.1.2 Who Should Use This Manual?

This manual is intended for the following users:

- Public Housing program users with Security Administration role

- Multifamily Housing program users with HQ User Administrator (HQA) role defined in WASS

- Multifamily Housing program users with HQ Security Administrator (HQS) role defined in WASS

- Multifamily Housing program users with Help Desk (HDK) role defined in WASS

If you have other roles or other action codes, you may need to access other documents in EIV library to learn more about them. For more information about the content of the EIV library, refer below to the *Related Documentation* section of this document.

This manual assumes the resources assigned to these roles have the following knowledge or expertise:

- Working knowledge of Microsoft Windows.

- Operational understanding of PC's.

- Operational understanding of Internet browsers.

- Understanding of basic network concepts.

- Understanding of HUD program terminology, policies, and procedures.

1.1.3 Related Documentation

This section provides a list of related documentation. The EIV library includes the following document:

- *EIV User Manual – For Public Housing Program Users* – For Public Housing program users of the EIV wage and income functionality, this manual provides step-by-step instructions. Users should be familiar with PCs, Microsoft Windows, and their browser software.

- *EIV User Manual – For Multifamily Housing Program Users* – For Multifamily Housing program users of the EIV benefit functionality, this manual provides step-by-step instructions. Users should be familiar with PCs, Microsoft Windows, and their browser software.

- *EIV User Administration Manual* – For Office of PIH and Multifamily Housing program user administrators, this manual provides step-by-step instructions on step-by-step instruction on the user administration available in EIV.

1.1.4 Abbreviations and Acronyms

A glossary of abbreviations and acronyms is included as **Appendix A** of this document.

2 Introduction

2 Introduction

EIV provides a portal to tenant income information in the form of household income data, as well as several income-based reports. EIV is a Web-based system, allowing access to information across secure Internet connections to the HUD application server using Microsoft Internet Explorer Version 6.0 and higher.

2.1 System Overview

The PIH and Office of Housing tenant income and benefits data in the EIV system come from a variety of sources:

1. **WASS** – provides user login information for single sign-on capability. Also provides the EIV Multifamily Housing program user's role profile.

2. **PIC Form 50058 Database** – provides navigational data to EIV and information to Form 50058 for PIH tenant (including MTW) and household information (Name, SSN, Program Type, Address, Projected Income, etc.).

3. **EIV Office of Housing Database** – provides information on Form 50059 (captured from TRACS) and the benefits information (captured from SSA) for the EIV Office of Housing tenants.

4. **NDNH** – provides wages reported by State and Federal Agencies, unemployment insurance income reported by State Agencies, and W-4 data reported by State and Federal Agencies to HHS/Office of Child Support Enforcement (OCSE) for PIH tenants.

5. **SSA** – provides benefit information including disability, supplemental income, and Social Security payments for PIH tenants.

EIV benefits data from SSA is updated on a quarterly cycle, with data for one-third of the states being in each monthly request. The monthly request also is augmented with information pertaining to new tenants (including newborns), portability move-in and those in PIC adjustment transactions.

Data exchange with the NDNH databases also follows a quarterly cycle for PIH wages and unemployment data but W-4 data is updated monthly and all data is collected monthly for new PIH tenants, household members who turn 18 (no data is collected from NDNH concerning those under 18), portability move ins and those in PIC adjustment transactions. EIV Release 5.0 does not collect income, employment and W-4 for Office of Housing tenants.

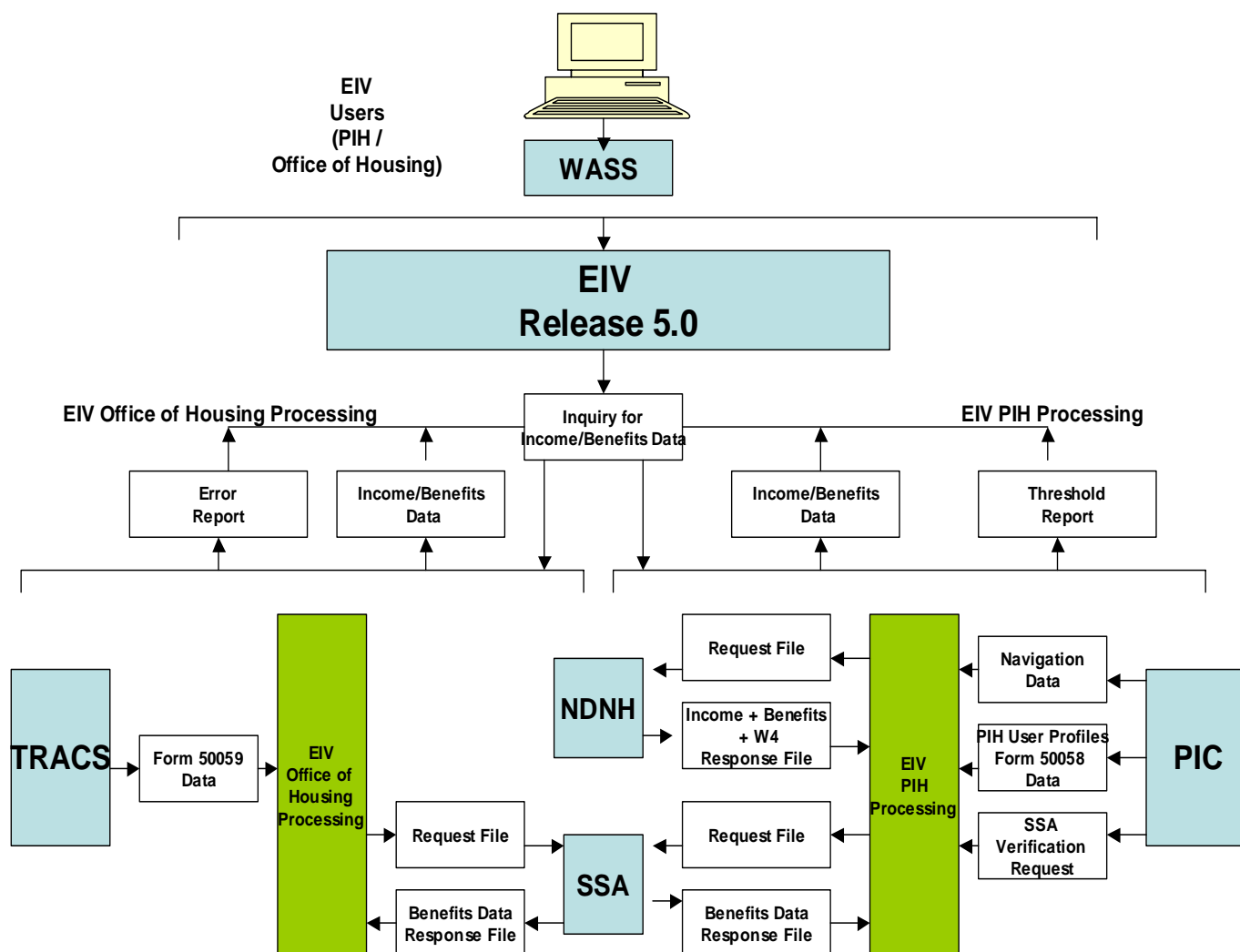**Figure 1** below illustrates the EIV data flow/system interfaces.

Figure 1 - EIV System Interfaces/Data Flow

2.2 Contingencies and Alternate Modes of Operation

EIV operates 24 hours a day, 7 days per week (except first weekend of each month due to PIC dependency). However, best conditions for use are during weekdays because batch processing will be run over night and during weekends, which may impact system responsiveness. **Notices of planned outages for system maintenance (as well as other guidance) will be posted on the EIV Information Web site**.

http://www.hud.gov/offices/pih/programs/ph/rhiip/uivsystem.cfm

2.3 Security

EIV contains personal information concerning tenants that is covered by the Privacy Act such as wage and income data about private individuals, as well as identifying information such as Social Security Number, address, and employment information. This information may only be used for limited official purposes, which are tenant recertification and oversight of the tenant recertification process (which includes use by OIG and GAO). It does not include sharing with governmental entities not involved in the recertification process. Users are encouraged to refer any non-standard requests for access to HUD management and to report any unauthorized disclosure of EIV data to the manager of the HUD Privacy Act Officer or to the Office of Inspector General. If it appears that the system has been "hacked", that should be reported to the HUD Help Desk (1-888-297-8689).

All EIV users must adhere to the Rules of Behavior outlined in the Appendix A of EIV System Security Plan. The rules clearly delineate responsibilities of, and expectations for, all individuals with access to the EIV system. Non-compliance with these rules will be disciplined through sanctions commensurate with the level of infraction. Sanctions against HUD staff may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination depending on the severity of the violation. Sanctions against HUD contractors may range from removal of system access for a specific period of time or indefinitely. Sanctions against HUD business partners may range from removal of system access for a specific period of time or indefinitely or if the violation is significant or persistent, the HUD business partner itself may lose access. Privacy Act violations may result in civil or criminal prosecution.

Access to tenant data is logged as part of the effort to protect the data and provide traceability should a questionable event occurs.

2.3.1 User Accounts

User accounts for EIV should be provided on a need-to-know basis, with appropriate approval and authorization. All EIV User Administrators are to maintain a file for each user with the access authorizations signed by the responsible manager and the EIV User Agreement signed by the user which include the EIV Rules of Behavior. User Administrators are required to certify each quarter that users have appropriate rights in EIV. They will be unable to make that certification if the documentation is not in the file. User accounts that have not been certified within 30 days thereafter will lose their EIV roles and will not be able to access EIV. User Administrators need to be able to confirm that the user roles need to be continued before making the certification. Contacting the supervisor of record in the file is the easiest way to do so.

EIV uses a role-based authorization scheme to grant Public Housing program users access to the EIV content. An EIV-Public Housing program user belongs to a security level based on their organization (Headquarters, Hub, TARC, Field Office, or PHA), and a role, based on their job responsibilities and functional needs.

- **Security level** – A user's access to data is limited to their organization level (Headquarters, Hub, TARC, Field Office, or PHA), and their specific organization.

    1. Headquarters user can see nationwide data.

    2. Hubs, TARCs, and Field Offices are still restricted to their respective areas.

    3. EIV supports the assignment of access to multiple PHAs under one WASS ID. Such an assignment will only be made to those PHA employees or contractors who access EIV and have a need documented in the User Administration file signed by the head of the additional PHA.

- **Role** – A role is an assigned right to use a distinct part of a system's functionality.

    EIV Public Housing program user roles include Occupancy Specialist, User Administrator, Systems Administrator and Security Administrator. A user's access to functionality is determined by the role or roles to which they are assigned. Each role provides access to a set of functions appropriate to that user type. For example, a PHA Occupancy Specialist can access income data features, but does not have access to user administration, security administration, or system administration features. A user can be assigned one or more roles; the functionality the user can access is a cumulative set of all features given to all roles to which the user is assigned. Users are assigned roles that are limited in scope to their organizational level. (PHA, Field Office, TARC, HUB, and Headquarters) and those below it.

    EIV utilizes the role-based and action code authorization scheme (as defined in WASS) to grant Multifamily Housing program users access to the EIV Office of Housing system content.

    The table below lists the Role Code and Action Code defined in WASS for Office of Housing Users.

Role Code	Role Description	Role Type	Action Code	Action Description
HQA	HQ User Administrator	I	UMT	User Maintenance
			VAR	View Audit Reports
HQU	HUD HQ User	I	VIR	View Income Reports
HQS	HQ Security Administrator	I	VAR	View Audit Reports
HDK	Helpdesk Personnel	I	UMT	User Maintenance
			VIR	View Income Reports
			VAR	View Audit Reports
HFU	HUD Field Office User	I	VIR	View Income Reports
HSU	Non-HUD User	E	VIR	View Income Reports
HCA	Contract Administrator	E	VIR	View Income Reports
HSC	Housing Coordinator	E	UMT	User Maintenance
			VIR	View Income Reports

2.3.2 Security Awareness

New EIV users are to receive as part of their training a familiarization with the requirements of the Privacy Act. Users are required to have annual security awareness training to refresh and update that initial training. Potential EIV users must sign the EIV Access Request to signify that they understand and accept the EIV Rules of Behavior. Guidance concerning security has been posted on the EIV web page.

http://www.hud.gov/offices/pih/programs/ph/rhiip/uivsystem.cfm

The complete text of the Privacy Act is available at:

http://www.usdoj.gov/foia/privstat.htm

2.3.3 Security Procedures

The WASS system, through which all users will access EIV, provides a timeout that disables access to the system after a 30-minute pause in use. That, in and of itself is not enough protection. Users should not leave their PC's unattended when access to WASS or any system accessible through WASS is possible. Users should be aware that logging out from EIV to WASS is not sufficient in that clicking on the WASS link to EIV will allow reentry to the EIV system. The activation of a screen saver is one way to protect access through an untended PC. Another is to close the browser window. It is possible to do so by going through the WASS closing routine which includes saying Yes to the question of whether to close the window. It is easier and quicker to close the browser window by clicking the X in the upper-right-hand corner of the screen.

Other security considerations relate to the physical security of the area where the EIV system is used, and policies and procedures that are enforced by management.

Guidance concerning security practices, governing the work area and storage of paper records containing personal information and their destruction when they no longer are needed, may be found at the EIV Information Web site.

2.3.4 Audits and User Activity Logging

Users of EIV are on notice that their activities and particularly tenant data access activities within the system are logged for security audit and reporting purposes. These reports will include records of successful access of sensitive data to which the user is authorized. It is the responsibility of the EIV Security Administrator to review logs regularly and reports (daily if possible) to identify suspicious patterns of behavior or to research patterns of behavior where suspicious behavior has occurred,.

Changes to the user roles and user certification transactions are also logged.

2.3.5 Standard Features

EIV provides the following standard features for security admin functions:

Pagination Capability
The reports available to EIV Security Administrators have pagination capability where search results are displayed in groups of 50 records (e.g., households, users) per page.

Where there are more than 50 records in the search results, the EIV have links to the other groups of 50 records through page number, which is in set of 10 pages. Navigation to next group of 10 pages, previous group of 10 pages, first page and last page of the search results are also provided to allow the user to access different sets of search results. The screen below illustrates the report pagination.

Required Fields

System Admin reports are generated based on the selection criteria fields. Fields marked with asterisk (*) are the fields required in order to generate the report. The screen below shows an example of required fields marked with asterisk.

3 Public Housing Program Security Administrators

3   PIH Security Administrators

The next sub-sections provide instructions on the EIV functions available to PIH Security Administrators.

3.1   User Role History Report

The User Role History Report module provide 2 options:

- *By User* – allows viewing of the role assignment history for any user

- *By User Administrator* – allows the viewing of role assignment activities performed by the user administrator.

3.1.1   User Role History Report - By User

To generate the User Role History Report – By User, follow these steps:
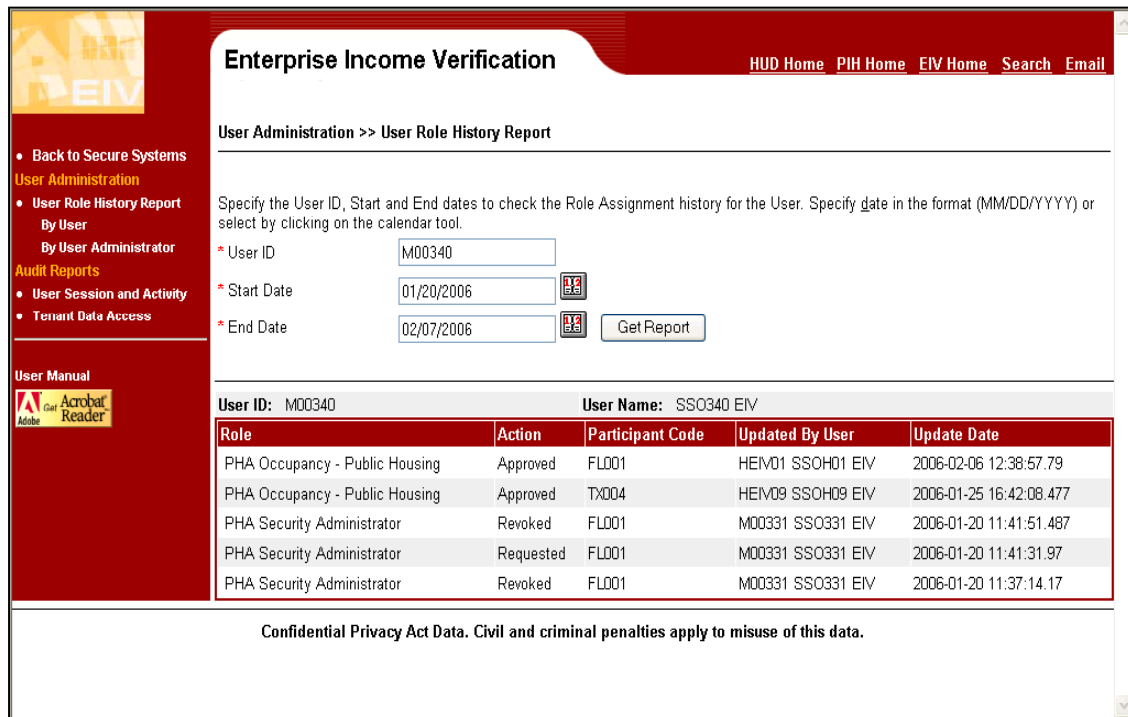
- Click the *By User* under the *User Role History Report* link in the left-hand navigation panel available to Public Housing program users.

The system displays the **User Administration - User Role History Report** page as shown below.

- Enter the **User ID**. Type in a date or click the **Calendar link** ( )

- Enter a date in the **Start Date and End Date** textboxes. Please note that the **Start Date** and **End Date** range should not exceed **30 days**.

- Click the **Get Report** button

The system displays the **User Administration - User Role History Report** page for the specified User within the specified **Start Date** and **End Date** as shown below.

The following fields are displayed on the report:

- Role

- Action

- Participant Code

- Updated by User

- Update Date

This report provides pagination capability as described in Section 2.3.5 of this document.

3.1.2 User Role History Report - By User Administrator

To generate the User Role History Report – By User Administrator, follow these steps:

- Click the *By User Administrator* under the *User Role History Report* link in the left-hand navigation panel available to Public Housing program user.

The system displays the **User Administration - User Role History Report** page as shown below.

- Enter the **User ID** of the **User Administrator**.

- Type in a date or click the **Calendar link** (⬛) and enter a date in the **Start Date and End Date** text boxes. Please note that the **Start Date** and **End Date** range should not exceed **30 days**.

- Click the **Get Report** button

The system displays the **User Administration - User Role History Report** page for the specified User Administrator within the specified **Start Date** and **End Date** as shown below.

The following fields are displayed on the report:

- Role

- Action

- Participant Code

- Updated User

- Update Date

This report provides pagination capability as described in Section 2.3.5 of this document.

3.2 Audit Reports

This chapter discusses the audit reporting functions in EIV. Audit reports allow the PIH Security Administrator to generate and review reports summarizing system and data use.

The following reports are discussed in this chapter:

- *User Session and Activity Audit Report*

- *Tenant Data Access Audit Report*

3.2.1 User Session and Activity Audit Report

This report details each user session and the pages accessed during the session. To view the User Session and Activity audit report, complete the following steps:

- Click the <u>User Session and Activity</u> link available to Public Housing program users

The system displays the **User Session and Activity Audit Report** page as shown below.

- Enter the **Report Date** in the format (MM/DD/YYYY), or select a date by clicking on the calendar ( ) tool.

- Click **Get Report**.

The system displays the **User Session and Activity Audit Report** results page as shown below.

This report provides pagination capability as described in Section 2.3.5 of this document.

3.2.2 Tenant Data Access Audit Report

This report provides a list of all EIV system users who have accessed the tenant wage and income data within a specified date range.

To view the Tenant Access audit report, complete the following steps:

- Click the Tenant Data Access link available to PIH Users

The system displays the **Tenant Data Access Audit Report** page as shown below.

- Enter **Start Date** in the format (MM/DD/YYYY), or select one by clicking on the calendar ([icon]) tool. The Start Date defines the beginning date for the reporting period. The Start Date value cannot be greater than the End Date value.

- Enter **End Date** in the format (MM/DD/YYYY), or select one by clicking on the calendar ([icon]) tool. The End Date defines the ending date for the reporting period. The End Date value must be greater than the Start Date value. . Please note that the **Start Date** and **End Date** range should not exceed **30 days**.

- Enter the **Tenant SSN** when you want to limit report content to a specific social security number. This is an optional field.

- Enter the **Tenant Last Name** when you want to limit report content to a specific tenant's name. This is an optional field.

- Select a **Participant Code** from the Participant Code drop down list to define the PHA code of the tenants to be included in the report.

- Click the **Get Report** button.

The system displays the **Tenant Data Access Audit Report** page as shown below.

The following fields are displayed on the report:

- User ID - the assigned access ID for a user

- User Name - the user's first and last name

- Activity - the identity of the PHA at which the activity tool place

- Date - the date and time the access was made

- Tenant Name - the tenant's name that was accessed

- SSN – the tenant's SSN that was accessed

- Reexamination Month - the Reexamination Month selected when searching of Income Information – By Reexamination Month

- Program Type - the type of housing project in which the tenant is participating, as applicable. It is also the Program Type selected when searching of Income Information – By Reexamination Month
- Project - the type of project in which the tenant is living, as applicable

The Tenant Data Access Report has sort icons that give the user control over the way the information in the report is displayed. Adjacent to the column title is a pair of triangular icons used for this sorting functionality. Clicking the top triangle will rearrange the column in an ascending order (A-Z), while clicking the bottom triangle will rearrange the column in a descending order (Z-A).

This report also provides pagination capability as described in Section 2.3.5 of this document.

To generate a printer-friendly version of the report,

- Click the Printer-friendly version link.

The system generates a printer-friendly version of the report and displays it in a separate Browser window.

- Click the Browser's print icon to produce a paper version of the report. When you have finished printing the report, close the browser window.

4 Multifamily Housing Program Security Administrators

4   Multifamily Housing Program Security Administrators

The next sub-sections provide instructions on the EIV functions available to Multifamily Housing Security Administrators.

4.1   Audit Reports

Audit reports allow the Office of Housing Security Administrator to generate and review reports summarizing the system and data use.

The following reports are discussed in this chapter:

- *User Session and Activity Audit Report*

- *Tenant Data Access Audit Report*

4.1.1   User Session and Activity Audit Report

This report details each user session and the pages accessed during the session. To view the User Session and Activity audit report, complete the following steps:

- Click the <u>User Session and Activity</u> link available to Multifamily Housing program users

The system displays the **User Session and Activity Audit Report** page as shown below.

- Enter the **Report Date** in the format (MM/DD/YYYY), or select a date by clicking on the calendar (⬛) tool.

- Click **Get Report** button

The system displays the **User Session and Activity Audit Report** results page as shown below.

This report provides pagination capability as described in Section 2.3.5 of this document.

4.1.2 Tenant Data Access Audit Report

This report provides a list of all EIV users who have access tenant wage and income data within a specified date range.

To view the Tenant Access audit report, complete the following steps:

- Click the Tenant Data Access link available to Multifamily Housing program users

The system displays the **Tenant Data Access Audit Report** page as shown below.

- Enter **Start Date** in the format (MM/DD/YYYY), or select one by clicking on the calendar (📅) tool. The Start Date defines the beginning date for the reporting period. The Start Date value cannot be greater than the End Date value.

- Enter **End Date** in the format (MM/DD/YYYY), or select one by clicking on the calendar (📅) tool. The End Date defines the ending date for the reporting period. The End Date value must be greater than the Start Date value. . Please note that the **Start Date** and **End Date** range should not exceed **30 days**.

- Enter the **Tenant SSN** when you want to limit report content to a specific social security number. This is an optional field.

- Click the **Get Report** button.

The system displays the **Tenant Data Access Audit Report** page as shown below.

The following fields are displayed on the report:

- User ID - the assigned access ID for a user

- User Name - the user's first and last name

- Date - the date and time the access was made

- SSN – the tenant's SSN that was accessed

- Recertification Month - the Recertification Month selected when searching Benefits Information by Subsidy Contract or By Project Number

- Contract - the Contract Number associated to the household

- Project Number - the Project Number associated to the household

This report provides pagination capability as described in Section 2.3.5 of this document.

5 Responsibilities of EIV Security Administrators

5 Responsibilities of EIV Security Administrators

The responsibility of EIV Security Administrators is to protect the integrity of the system.
.

5.1 Purpose of Reports

The purpose of the reports that are available to EIV Security Administrators is to help them identify if there may be a situation wherein a user is abusing his/her system access to use the information for private purposes, perhaps to misuse identify information or to sell it.

5.2 Role of the EIV Security Administrator

EIV Security Administrators are not expected to be investigators or to make accusations. If there is reason to think that the EIV system is being abused, that access to information is being used for improper purposes, to protect the integrity of system, the Security Administrator should report the facts to the Office of Inspector General. If the facts are not clear, the EIV Security Administrators may consult with counterparts, the Headquarters EIV Security Administrator or experts in the Headquarters program office and then report the facts to the Office of Inspector General if appropriate.

5.3 The Need to Avoid Conflict of Interest

Guidance from the National Institute of Standards and Technology, which sets Federal security standards, is that security personnel should avoid serving in other roles for the same system. The purpose of that guidance is to help assure that security personnel do not have a conflict of interest in being responsible for monitoring the very functions that they may monitor. This is particularly a potential problem in serving as both EIV User Administrator and EIV Security Administrators. That is because while EIV is not a transactional system, the User Administrators are ones who perform transactions in EIV. EIV Security Administrators are responsible for monitoring those same transactions.

APPENDIX A - ABBREVIATIONS AND ACRONYMS

The following abbreviations, and acronyms may or may not appear in this document.
They are provided for reference and clarity.

Acronym	Definition
C&A	Certification and Accreditation
CAN	Claim Account Number
CCB	Change Control Board
CCMB	Configuration Change Management Board
CM	Configuration Management
CMRB	Contract Management Review Board
COTR	Contracting Officer's Technical Representative
DCG	Development Coordination Group
DRP	Disaster Recovery Plan
DTS	Data Transmission Services
EDI	Electronic Data Interchange
EIV	Enterprise Income Verification
FEIN	Federal Employer Identification Number
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FO	Field Office
FOIA	Freedom of Information Act
Form HUD-50058	Form used to submit resident characteristics and tenant income data to HUD
FOUO	For Official Use Only
FTP	File Transfer Protocol
GTM	Government Technical Monitor
GTR	Government Technical Representative
HHS	U.S. Department of Health and Human Services
HOH	Head of Household
HOUSING	Office of Housing - FHA
Hub	Not an acronym. FO is classified into two categories -- Hub and Program Center. A Hub can be a stand-alone FO or have another office, a Program Center, report to it.
HUD	US Department of Housing and Urban Development
ICN	Income Control Number
MOA/U	Memorandum of Agreement / Understanding
MTW	Moving To Work
NDNH	National Directory of New Hires
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPC	Office of Procurement & Contracts
PD&R	HUDs Office of Policy, Development and Research
PHA	Public Housing Authorities
PI	Period of Income

Acronym	Definition
PIA	Privacy Act Assessment
PIC	Public & Indian Housing Information Center
PIH	HUD's Office of Public & Indian Housing
POA&M	Plan of Action and Milestones
PVCS	Project Version Control System
PWS	Performance Work Statement
QA	Quality Assurance
QU	Quarterly Update
QW	Quarterly Wage
RHIIP	Rental Housing Integrity Improvement Project
RIM	Rental Integrity Monitoring
SEIN	State Employment Identification Number
SPH	HUD's Security Program Handbook
SPP	Security Program Policy
SS	Social Security
SSA	Social Security Administration
SSAA	System Security Authorization Agreement
SSI	Supplemental Security Income
SSO	Single Sign On (used in WASS)
SSP	System Security Plan
TARC	Troubled Agency Recovery Center
TASS	Tenant Assessment Subsystem
TRACS	Tenant Rental Assistance Certification System
TTP	Total Tenant Payment
V V&T	Verification, Validation, & Test
W-4	New Hires data
WASS	Web Access Security Subsystem